CLAIMS

[c1] 1. An authentication apparatus operable to produce a secure identifier, the apparatus comprising:

a processor;

a clock coupled to the processor configurable to generate a time element;

a memory element coupled to the processor configurable to store a private key and public key information;

at least one actuator coupled to the processor;

a signature generator coupled to the processor operable to generate a digital signature, the digital signature being a function of the private key and the time element; and

an emitter coupled to the signal generator operable to emit the secure identifier, the secure identifier comprising the digital signature, time element, and public key information.

[c2] 2. The apparatus set forth in Claim 1, the signature generator further comprising:

a random number generator coupled to the processor to encrypt the digital signature.

[c3] 3. The apparatus set forth in Claim 1, wherein the time element comprises a predetermined number of least significant bits of the time.

[c4] 4. The apparatus set forth in Claim 1, further comprising an input element coupled to the processor, the input element capable of receiving a personal identification number (PIN).

[c5] 5. The apparatus set forth in Claim 1, further comprising an input element coupled to the processor, the input element capable of receiving a challenge.

[c6] 6. The apparatus set forth in Claim 1, further comprising a display coupled to the processor, the display capable of displaying key identifiers.

[c7] 7. The apparatus set forth in Claim 1, wherein the secure identifier emitted is emitted as an audio tone.

[c8] 8. The apparatus set forth in Claim 1, wherein the secure identifier emitted is emitted as an optical signal.

[c9] 9. The apparatus set forth in Claim 1, wherein the actuator is a push-button switch.

[c10] 10. The apparatus set forth in Claim 1, wherein the actuator is a voice activated switch.

[c11] 11. The apparatus set forth in Claim 1, wherein the public key information is a public key identifier.

[c12] 12. The apparatus set forth in Claim 11, wherein the pubic key identifier is derived from the public key information.

[c13] 13. The apparatus set forth in Claim 1, wherein the public key information is the public key.

[c14] 14. The apparatus set forth in Claim 1, wherein the digital signature is encrypted using a personal identification number (PIN).

[c15] 15. A method of authenticating, comprising:

generating a time element;

identifying a key identifier;

generating a digital signature;

generating a secure identifier as a function of the time element, the key identifier, the digital signature; and

emitting the secure identifier.

[c16] 16. The method set forth in Claim 15, further comprising identifying a PIN, and wherein generating a digital signature is further a function of the PIN.

[c17] 17. The method set forth in Claim 15, wherein the secure identifier emitted is emitted as an audible tone.

[c18] 18. The method set forth in Claim 15, wherein the secure identifier emitted is emitted as an optical signal.

[c19] 19. The method set forth in Claim 15, wherein the digital signature is derived from a private key.

[c20] 20. An authentication receiver, comprising:

a receiver configurable to receive a secure identifier, the secure identifier comprising:

a digital signature, the digital signature comprising information derived from a private key,

a public key identifier; and

a time identifier; and

a verifier configurable to verify the secure identifier, the verifier comprising:

memory comprising information corresponding to the public key information received and time tolerance information;

a key retriever coupled to the memory and configurable to retrieve a public key corresponding to the public key identifier; and

a time verifier coupled to the memory and configurable to verify that the received time identifier falls within acceptable time tolerances.

[c21] 21. The apparatus set forth in Claim 20, the secure identifier further comprises a PIN, and wherein the receiver is configurable to decrypt the digital signature using the PIN.

[c22] 22. The apparatus set forth in Claim 20, wherein the key retriever compares the public key identifier received to public key information stored in memory.

[c23] 23. The apparatus set forth in Claim 20, wherein the time tolerance information comprises information regarding clock drift.

[c24] 24. The apparatus set forth in Claim 20, wherein the secure identifier is emitted as an audible tone.

[c25] 25. The apparatus set forth in Claim 20, wherein the secure identifier is emitted as an optical signal.

[c26] 26. A method of authenticating, comprising:

receiving a secure identifier, the secure identifier comprising a digital signature, a key identifier, and a time identifier; and

verifying the secure identifier, verifying comprising:

verifying that the public key identifier received corresponds to known information regarding the public key identifier received; and

verifying the time identifier such that the time identifier received is within predetermined time tolerances.

[c27] 27. The method set forth in Claim 26, the digital signature further comprises a PIN, and where receiving further comprises decrypting at least a portion of the digital signature using the PIN.

[c28] 28. The method set forth in Claim 26, wherein the secure identifier received is received as an audible tone.

[c29] 29. The method set forth in Claim 26, wherein the secure identifier received is received as an optical signal.

[c30] 30. An authentication apparatus operable to produce a secure identifier, the apparatus comprising:

a processor means;

a clock means coupled to the processor configurable to generate a time element;

a memory element means coupled to the processor means configurable to store a private key means and public key information means;

at least one actuator means coupled to the processor means;

a signature generator means coupled to the processor means operable to generate a digital signature means, the digital signature means being a function of the private key means and the time element means; and

an emitter means coupled to the signal generator means operable to emit the secure identifier, the secure identifier comprising the digital signature, time element, and public key information.

[c31] 31. The apparatus set forth in Claim 30, the signature generator means further comprising:

a random number generator means coupled to the processor means to encrypt the digital signature means.

[c32] 32. The apparatus set forth in Claim 30, wherein the time element means comprises a predetermined number of least significant bits of the time.

[c33] 33. The apparatus set forth in Claim 30, further comprising an input element means coupled to the processor means, the input element means capable of receiving a personal identification number (PIN) means.

[c34] 34. The apparatus set forth in Claim 30, further comprising an input element means coupled to the processor means, the input element means capable of receiving a challenge means.

[c35] 35. The apparatus set forth in Claim 30, further comprising a display means coupled to the processor means, the display means capable of displaying at least one key identifier means.

[c36] 36. The apparatus set forth in Claim 30, wherein the secure identifier means emitted is emitted as an audio tone means.

[c37] 37. The apparatus set forth in Claim 30, wherein the secure identifier means emitted is emitted as an optical signal means.

[c38] 38. The apparatus set forth in Claim 30, wherein the actuator means is a push-button switch.

[c39] 39. The apparatus set forth in Claim 30, wherein the actuator means is a voice activated switch.

[c40] 40. The apparatus set forth in Claim 30, wherein the public key information means is a public key identifier means.

[c41] 41. The apparatus set forth in Claim 40, wherein the pubic key identifier means is derived from the public key information means.

[c42] 42. The apparatus set forth in Claim 30, wherein the public key information is the public key.

[c43] 43. The apparatus set forth in Claim 30, wherein the digital signature means is encrypted using a personal identification number (PIN) means.

[c44] 44. A method of authenticating, comprising:

means for generating a time element;

means for identifying a key identifier;

means for generating a digital signature;

means for generating a secure identifier as a function of the time element, the key identifier, the digital signature; and

means for emitting the secure identifier.

[c45] 45. The method set forth in Claim 44, further comprising means for identifying a PIN, and wherein means for generating a digital signature is further a function of the PIN.

[c46] 46. The method set forth in Claim 44, wherein the secure identifier emitted is emitted as an audible tone.

[c47] 47. The method set forth in Claim 44, wherein the secure identifier emitted is emitted as an optical signal.

[c48] 48. The method set forth in Claim 44, wherein the digital signature is derived from a private key.

[c49] 49. An authentication receiver, comprising:

a receiver means configurable to receive a secure identifier means, the secure identifier means comprising:

a digital signature means, the digital signature means comprising information derived from a private key means, a public key identifier means; and

a time identifier means; and

a verifier means configurable to verify the secure identifier means, the verifier means comprising:

memory means comprising information corresponding to the public key information means received and time tolerance information means;

a key retriever means coupled to the memory means and configurable to retrieve a public key means corresponding to the public key identifier means; and

a time verifier means coupled to the memory means and configurable to verify that the received time identifier means falls within acceptable time tolerances.

[c50] 50. The apparatus set forth in Claim 49, the secure identifier means further comprises a PIN means, and wherein the receiver is configurable to decrypt the digital signature means using the PIN means.

[c51] 51. The apparatus set forth in Claim 49, wherein the key retriever means compares the public key identifier means received to public key information means stored in memory.

[c52] 52. The apparatus set forth in Claim 49, wherein the time tolerance information comprises information regarding clock drift.

[c53] 53. The apparatus set forth in Claim 49, wherein the secure identifier means is emitted as an audible tone.

[c54] 54. The apparatus set forth in Claim 49, wherein the secure identifier means is emitted as an optical signal.

[c55] 55. A method of authenticating, comprising:

means for receiving a secure identifier, the secure identifier comprising a digital signature, a key identifier, and a time identifier; and

means for verifying the secure identifier, verifying comprising:

means for verifying that the public key identifier received corresponds to known information regarding the public key identifier received; and means for verifying the time identifier such that the time identifier received is within predetermined time tolerances.

[c56] 56. The method set forth in Claim 55, the digital signature further comprises a PIN, and where means for receiving further comprises decrypting the digital signature using the PIN.

[c57] 57. The method set forth in Claim 55, wherein the secure identifier received is received as an audible tone.

[c58] 58. The method set forth in Claim 55, wherein the secure identifier received is received as an optical signal.